REMARKS/ARGUMENTS

Prior to this amendment, claims 1-8, 10-19, 21-29 and 31-36 were pending. In this amendment, claims 1 and 36 are amended, claim3 is canceled, and claims 37-38 are added. No new matter is added. Thus, after entry of this amendment, claims 1-8, 10-19, 21-29, and 31-38 are pending.

I. Examiner Interview

On January 29, 2009, a telephonic interview was held between the Examiner and the undersigned. During the interview the claims in light of the references was discussed. The undersigned thanks the Examiner for his time and consideration of the arguments presented.

II. Claim Rejections – 35 U.S.C. § 102(b) and § 103(a) Hodgson

Claims 1-8, 10-19, 21-29, and 31-36 are rejected under 35 U.S.C. 102(b) as being anticipated by, or in the alternative, under 35 U.S.C. 103(a) as obvious over Hodgson et al. (U.S. Patent Pub. No. 2002/0123972)("*Hodgson*"). This rejection is traversed.

Anticipation has not been established because each and every limitation is not taught by *Hodgson*. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). MPEP 2131.

Obviousness has not been established because the Office Action has not made a prima facie case of obviousness. "The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1396 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some

rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). See also *KSR*, 550 U.S. at ___, 82 USPQ2d at 1396 (quoting Federal Circuit statement with approval)." MPEP 2142.

Claim 1

Claim 1 is amended to incorporate the limitations in previously dependent claim 3. Each and every limitation of claim 1 is not disclosed or suggested by *Hodgson*. For example, claim 1 recites in part, "*an Access Control Server (ACS) configured to receive a request for passcode authentication of a Primary Account Number (PAN) from a merchant server, and configured to request a passcode corresponding to the PAN from a cardholder device, wherein the ACS is associated with an issuer of the PAN.*" The Office Action cites P[0090] and Figure 2A, step 210 of *Hodgson* as disclosing the ACS. (Office Action Pg. 4). The Office Action is unclear as to which elements in *Hodgson* are being equated with the elements in claim 1, however this is inconsequential, as no reasonable interpretation of *Hodgson* discloses or suggests all of the limitations of claim 1. For the Examiner's convenience, Fig. 1A of *Hodgson* is reproduced below.

A. ***STMS is interpreted as being the Access Control Server***

One interpretation of *Hodgson,* which the Examiner indicated was his interpretation during the Examiner interview, may equate the STMS (Fig. 1A, 30) with the Access Control Server (ACS). However, under this interpretation, *Hodgson* does not disclose or suggest "*an Access Control Server (ACS) configured to receive a request for passcode authentication of a Primary Account Number (PAN) from a merchant server.*" As should be clear from Fig. 1A below, the STMS (30) does not communicate with the Merchant Server (20), as there are no arrows indicating communications between STMS (30) and Merchant Server (20). As such, the STMS (30) does not receive anything from the Merchant Server (20) including a request for passcode authentication.

Furthermore, this interpretation of *Hodgson* does not disclose or suggest an Access Control Server "*configured to request a passcode corresponding to the PAN from a cardholder device.*" Again referring to Fig 1A, *Hodgson* contains two arrows, 3 and 6, depicting communication between the STMS (30) and a cardholder device (12, 16). Arrow 3 is described as the cardholder device encrypting a PIN and sending it to the STMS (30). (*Hodgson* P[0076]). The STMS (30) does not request the PIN be sent. Arrow 6 is described as the STMS (30) returning a response to the cardholder device (12,16) indicating a transaction is approved. (*Hodgson* P[0081-0084]). The response message does not request a PIN from the cardholder device, but rather informs the cardholder device the transaction has been approved. Neither of these two interactions disclose or suggest an Access Control Server requesting a passcode.

Finally, this interpretation of *Hodgson* does not disclose or suggest "*wherein the ACS is associated with an issuer of the PAN.*" Although Fig. 12 of *Hodgson* may depict Issuing Banks (Fig. 12, 1250, 1270), there is no association between the issuing banks and the STMS (30). As such, using the interpretation of the STMS as an access control server fails to disclose or suggest each and every limitation of claim 1. Furthermore, the Office Action has articulated no reasoning as to why it would be obvious to modify *Hodgson* to contain such limitations and has failed to make a prima facie case as to why such modifications would be obvious.

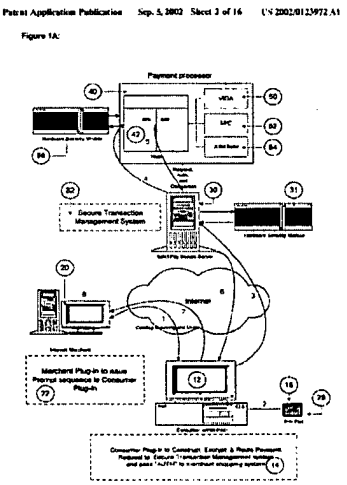
B. *User Computer is interpreted as being the Access Control Server*

An alternative interpretation of *Hodgson*, which the Examiner did not indicate was his interpretation, may equate the Access Control Server with the user computer (16). Under this interpretation, the user computer (12) may receive a request for passcode authentication from a merchant server (20). (Arrow 1, P[0066-0068]). The user computer may also request a passcode from a cardholder device (PinPad 16). (Arrow 2, P[0070-0072]). However, this interpretation fails to disclose or suggest "*wherein the ACS is associated with an issuer of the PAN.*" If the ACS is equated with the user computer (16), *Hodgson* does not disclose or suggest the user computer (16) being associated with the issuer of the PAN. Again, although Fig. 12 of *Hodgson*

may depict Issuing Banks (Fig. 12, 1250, 1270), there is no association between the issuing banks and the user computer (12).

Furthermore, under this interpretation, the user computer (12), which is being equated to the ACS, may request a passcode from the cardholder device (PinPad 16). In such an interpretation, the cardholder device is the PinPad (16). However, claim 1 further contains the limitation, "*a front end Hardware Security Module (HSM) coupled to the ACS.*" Reviewing figure 1A, the user computer (12) (ACS) is only coupled to the PinPad(16). However, the PinPad (16) has already been equated to the cardholder device. *Hodgson* does not teach or suggest "*a front end Hardware Security Module (HSM) coupled to the ACS.*" As such, using the interpretation of the user computer as an access control server fails to disclose or suggest each and every limitation of claim 1. Furthermore, the Office Action has articulated no reasoning as to why it would be obvious to modify *Hodgson* to contain such limitations and has failed to make a prima facie case as to why such modifications would be obvious.

The Office Action has failed to show that the limitations of claim 1 are anticipated, or in the alternative, obvious over *Hodgson* for the reasons set forth above. Withdrawal of the rejection of claim 1, and the claims which depend therefrom, is respectfully requested.



Claim 16

Claim 16 is not amended. Each and every limitation of claim 16 is not disclosed or suggested by *Hodgson.* For example, claim 16 recites in part, an Access Control Server "*configured to generate a request for a PIN corresponding to the PAN.*" The Office Action on page 7 has equated the Access Control Server with the STMS. As explained above with respect to claim 1, if the Access Control Server is considered the ACS, *Hodgson* fails to disclose or suggest the STMS requesting a PIN.

In the alternative, if the Access Control Server is equated to the consumer's computer, the request for a PIN would be the consumer's computer instructing the user to enter his pin into the PinPad. However, such an interpretation fails to disclose or suggest "*the request for the PIN including hidden fields comprising a unique transaction identifier and a hash value,*" because the instructions to the user to enter a PIN do not include hidden fields or a transaction identifier. (*Hodgson* P[0070-0075]).

Furthermore, the Office Action has articulated no reasoning as to why it would be obvious to modify *Hodgson* to contain such limitations and has failed to make a prima facie case as to why such modifications would be obvious. The Office Action has failed to show that the limitations of claim 16 are anticipated, or in the alternative, obvious over *Hodgson* for the reasons set forth above. Withdrawal of the rejection of claim 16, and the claims which depend therefrom, is respectfully requested.

Claim 18

Claim 18 is not amended. Each and every limitation of claim 18 is not disclosed or suggested by *Hodgson.* Claim 18 contains limitations that are not disclosed or suggested by *Hodgson* for reasons including those set forth above with respect to claim 16. Furthermore, *Hodgson* does not teach or suggest "*the request for the PIN including an instruction to provide the PIN to a destination address.*" The Office Action alleges this is disclosed in *Hodgson* P[0087], which recites:

> The ***STMS*** 30 automatically sends a follow-up email to the email addressed used to register the PIN/PAD 16. The email contains the transaction information as a confirmation for the consumer.

(*Hodgson* P[0087]). *Hodgson* describes an e-mail being sent to the user after a transaction is completed, such that the user is informed that a purchase was made. The Office Action has alleged that the e-mail address as described in *Hodgson* is the destination address. (Office Action Pg. 8). Under this interpretation, the request for the PIN would include an instruction for the PIN to be sent to the user's e-mail address. Such a construction would render *Hodgson* inoperable, because if the PIN is sent to the user's e-mail address instead of the STMS, the STMS will not be able to process the transaction because it would be lacking the PIN.

Further more, claim 18 recites "*a front end Hardware Security Module (HSM) having said destination address.*" Using the Office Action's interpretation of a destination address would require the a hardware security module to not only have an e-mail address, it would have to have the e-mail address of the user. *Hodgson* does not teach or suggest a hardware security module with any e-mail address let alone the e-mail address of the user. Furthermore, providing an e-mail address for a hardware security module would be nonsensical, as a piece of hardware would not have an e-mail address.

The Office Action has articulated no reasoning as to why it would be obvious to modify *Hodgson* to contain such limitations and has failed to make a prima facie case as to why such modifications would be obvious. The Office Action has failed to show that the limitations of claim 18 are anticipated, or in the alternative, obvious over *Hodgson* for the reasons set forth above. Withdrawal of the rejection of claim 18, and the claims which depend therefrom, is respectfully requested.

Claim 19

Claim 19 is not amended. Each and every limitation of claim 18 is not disclosed or suggested by *Hodgson.* For example, claim 19 recites in part, "*requesting a Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN) wherein requesting the PIN includes generating a unique transaction identifier, generating a hash value with a front end Hardware Security Module (HSM) based in part on the unique transaction*

identifier, generating a query having the unique transaction identifier and hash value as fields in the query, and communicating the query." There are only two places in *Hodgson* where a PIN is requested. The first is the merchant framework sending a HTML page to the user to instruct the user to enter his PIN. (*Hodgson* P[0070-0072]). The second is where the consumer computer receives the HTML page and processes the page to instruct the user to enter his PIN into the PinPad. (*Hodgson* P[0069-0075]).

With respect to the first request for a PIN, *Hodgson* does not disclose or suggest a hardware security module at the merchant site. As such, it is not possible for the request for a PIN generated at the merchant site to include "*generating a hash value with a front end Hardware Security Module (HSM).*" With respect to the second request for a PIN, *Hodgson* does not disclose the PinPad "*generating a hash value with a front end Hardware Security Module (HSM) based in part on the unique transaction identifier.*" Although *Hodgson* may disclose the PinPad encrypting the credit card number / PIN, encryption and hashing are not the same thing. Encryption ensures privacy, while a hash ensures authenticity. Even if encryption and hashing are considered the same thing, *Hodgson* does not disclose or suggest the credit card number / PIN is encrypted "*based in part on the unique transaction identifier.*"

The Office Action has articulated no reasoning as to why it would be obvious to modify *Hodgson* to contain such limitations and has failed to make a prima facie case as to why such modifications would be obvious. The Office Action has failed to show that the limitations of claim 19 are anticipated, or in the alternative, obvious over *Hodgson* for the reasons set forth above. Withdrawal of the rejection of claim 19, and the claims which depend therefrom, is respectfully requested.

Claim 28

Claim 28 is not amended. Each and every limitation of claim 28 is not disclosed or suggested by *Hodgson*. For example, claim 28 recites in part:

> **receiving an encrypted Personal Identification Number** (PIN) corresponding to a Primary Account Number (PAN) **in a front end Hardware Security Module** (HSM) over a Secured Sockets Layer (SSL) internet connection between a cardholder device and the front end HSM, wherein **the PIN is exclusively SSL encrypted**;

(emphasis added). *Hodgson* does not disclose receiving an encrypted PIN in a front end HSM wherein the PIN is exclusively SSL encrypted. *Hodgson* does describe SSL encryption, however it describes SSL encryption of the PIN as an additional encryption, not an exclusive encryption. *Hodgson* states:

> At arrow 3), software causes the browser to **further encrypt** the message with 128bit SSL and **transmit it directly to STMS** 30 (see FIG. 9).

(*Hodgson,* P[0076], *emphasis added).* As such, *Hodgson* does not disclose "*the PIN is exclusively SSL encrypted.*" Furthermore, *Hodgson* states the encrypted PIN is transmitted directly to the STMS. The STMS is not a hardware security module. As such, *Hodgson* does not disclose receiving an encrypted PIN over a SSL connection "*in a front end hardware security module.*"

The Office Action has articulated no reasoning as to why it would be obvious to modify *Hodgson* to contain such limitations and has failed to make a prima facie case as to why such modifications would be obvious. The Office Action has failed to show that the limitations of claim 28 are anticipated, or in the alternative, obvious over *Hodgson* for the reasons set forth above. Withdrawal of the rejection of claim 28, and the claims which depend therefrom, is respectfully requested.

Claim 32

Claim 32 is not amended. Each and every limitation of claim 32 is not disclosed or suggested by *Hodgson.* For example, claim 32 recites in part "*receiving in a front end Hardware Security Module (HSM) an encrypted PIN and at least a portion of the encryption data from the cardholder in response to the query.*" *Hodgson* does not disclose or suggest receiving an encrypted PIN from a cardholder in a front end hardware security module in response to a query for the PIN. *Hodgson* describes sending an HTML page to a consumer's computer to request a payment. (*Hodgson* P[0068]). *Hodgson* further describes the HTML page instructing the consumer to swipe their credit card into a PinPad, and enter a PIN. (*Hodgson* P[0073]). This is the only place in *Hodgson* where a consumer enters his PIN, and when he enters it into the

PinPad, he is not entering the PIN in an encrypted format. As such, if the PinPad is considered the front end HSM, it does not receive an encrypted PIN "*from the cardholder.*" Furthermore, any of the other HSMs described in *Hodgson* do not receive input from the cardholder, but rather receive input from the STMS or a Payment Processor. (*Hodgson,* Fig. 1A).

The Office Action has articulated no reasoning as to why it would be obvious to modify *Hodgson* to contain such limitations and has failed to make a prima facie case as to why such modifications would be obvious. The Office Action has failed to show that the limitations of claim 28 are anticipated, or in the alternative, obvious over *Hodgson* for the reasons set forth above. Withdrawal of the rejection of claim 32, and the claims which depend therefrom, is respectfully requested.

Claim 36

Claim 36 has been rewritten in independent form. No new matter has been added. Claim 36 is allowable for at least the reasons as set forth with respect to claim 32. Furthermore, claim 36 contains several limitations that are not disclosed or suggested by *Hodgson.* For example, *Hodgson* does not disclose or suggest encryption data comprising a base redirection url. Withdrawal of the rejection of claim 36 is respectfully requested.

III. Newly added claims 37-38

Claims 37-38 are added. Support for claim 37 can be found throughout the specification including such places as P[0074]. Claims 37 is patentably distinct over *Hodgson* because the ACS, front end HSM, and back end HSM being co-located is not disclosed or suggested in *Hodgson.* Support for claim 38 can be found throughout the specification including such places as P[0056]. Claims 38 is patentably distinct over the cited reference because an ACS returning an authentication response to the merchant server is not disclosed or suggested in *Hodgson.*

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

/Preetam B. Pagar/

Preetam B. Pagar
Reg. No. 57,684

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
PBP:scz
61781106 v1